Remarks of Lydia B. Parnes
ABA Spring Meeting
Breakfast with the Bureau Directors
April 20, 2007

I. Introduction

Thank you, Christine. I am pleased to be here for my third ABA Breakfast with the Bureau Directors. For the past two years, I've talked generally about our consumer protection priorities. As consumers, I hope you appreciate the importance of this work, but, as practitioners, you may wonder how it affects you. So today, I would like to focus on a few areas of BCP's mission that your clients should care about – data security, spyware, and health advertising.

Since all of these topics have been in the headlines in recent months, the theme for my talk will be "consumer protection in the news" – with tips on counseling your clients so that they can avoid becoming the next consumer protection headline.

II. Data Security and Identity Theft

Obviously, data security and identity theft have been prominent in the headlines over the past several months.

Let's say a client of yours, an owner of a retail chain, has been following these headlines. The client walks into your office and says, "I keep my customers' credit card information, but not their social security numbers. Do I have a legal obligation to safeguard this data?" Your answer should be a resounding yes.

What is the legal standard that applies to this retailer? If your client is a bank, it would be covered by the Gramm-Leach-Bliley Act, which contains safeguards requirements for financial

institutions.[1] If it is a credit bureau, it would be covered by the Fair Credit Reporting Act, which includes "know your customer" requirements for consumer reporting agencies.[2] But, as a retailer, the client is covered by the FTC Act's prohibition against "unfair or deceptive acts or practices."[3] Whether a financial institution, credit reporting agency, or retailer, the basic standard is the same: Companies must maintain reasonable and appropriate measures to protect sensitive consumer information.

What does the "reasonableness" standard mean in practice? The FTC has brought 14 law enforcement actions against businesses that have failed to provide reasonable data security.[4] These enforcement actions can provide some lessons for your clients.

First, if you make claims about data security, be sure that they are accurate. In actions against Microsoft,[5] Petco,[6] and Tower Records,[7] the FTC challenged claims on the companies' websites that each had strong security procedures in place to protect consumer information. The FTC alleged that, contrary to these claims, the companies did not have even the most basic security measures in place.

---

[1] 15 U.S.C., §§ 6801-6809.

[2] 15 U.S.C. § 1681 et seq.

[3] 15 U.S.C. § 45(a).

[4] *See generally* FTC Privacy Initiatives, *available at* http://www.ftc.gov/privacy.

[5] *See* FTC Press Release, *Microsoft Settles FTC Charges Alleging False Security and Privacy Promises* (August 8, 2002), *available at* http://www.ftc.gov/opa/2002/08/microsoft.shtm.

[6] *See* FTC Press Release, *Petco Settles FTC Charges; Security Flaws Allowed Hackers to Access Consumers' Credit Card Information* (November 17, 2004), *available at* http://www.ftc.gov/opa/2004/11/petco.shtm.

[7] *See* FTC Press Release, *Tower Records Settles FTC Charges; Security Flaw Allegedly Exposed Customers' Personal Information to Other Web Users* (April 21, 2004), *available at* http://www.ftc.gov/opa/2004/04/towerrecords.shtm.

Second, be aware of well-known and common security threats and protect against them. In many of our cases, we alleged that companies failed to protect their customer information from a simple and well-known type of hacker attack.[8] In others, we have challenged failures to protect data from obvious low-tech security threats such as dumpster diving.[9]

Third, know with whom you are sharing your customers' sensitive information. Perhaps our most well-known security case was against ChoicePoint, which sold 160,000 consumer files to identity thieves posing as clients. In its complaint, the Commission alleged that ChoicePoint lacked reasonable procedures to verify the legitimacy of its customers.[10]

Fourth, do not retain sensitive consumer information that you do not need. In cases we announced last year against BJ's Warehouse[11] and DSW,[12] the companies stored full magnetic stripe information unnecessarily – long after the time of the transaction, when the companies no longer had a business need for the information. The magnetic stripe information was unencrypted

---

[8] *See* e.g., FTC Press Release, *Guidance Software; Company Failed to Use Reasonable Security Measures to Protect Consumers' Data* (November 16, 2006), *available at* http://www.ftc.gov/opa/2006/11/guidance.shtm.

[9] *See* FTC Press Release, *Real Estate Services Company Settles Privacy and Security Charge; Company Tossed Consumers' Confidential Information in Dumpster; Company Computers were Hacked* (May 10, 2006), *available at* http://www.ftc.gov/opa/2006/05/nationstitleemailtest.shtm.

[10] *See* FTC Press Release, *ChoicePoint Settles Data Security Breach Charges; To Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress* (Jan. 26, 2006), *available at* http://www.ftc.gov/opa/2006/01/choicepoint.htm. In settling the matter, ChoicePoint agreed to pay a $10 million penalty and another $5 million to compensate identity theft victims. The Commission has mailed more than 1,400 claims forms to possible victims and has created a website where consumers can download claims forms and obtain information about the claims process.

[11] *See* FTC Press Release, *BJ's Wholesale Club Settles FTC Charges; Agency Says Lax Security Compromised Thousands of Credit and Debit Cards* (June 16, 2005), *available at* http://www.ftc.gov/opa/2005/06/bjswholesale.shtm.

[12] *See* FTC Press Release, *DSW Inc. Settles FTC Charges; Agency Says Company Failed to Protect Sensitive Customer Data* (December 1, 2005), *available at* http://www.ftc.gov/opa/2005/12/dsw.shtm.

and had weak access controls. As a result, thieves were able to hack into a single store's database and from there into the company's central database, where they obtained hundreds of thousands of credit card numbers and security codes.

These are the types of things you might tell your retailer client. You can also provide your client with a business education brochure we recently developed that articulates five key steps of a sound data security plan. We think the brochure will be a useful tool in alerting businesses to the importance of data security issues and give them a solid foundation on how to address those issues. The guide has been included in the "Business Briefcase" CD-Rom that I have handed out to you today.

III. Spyware

Another topic that has been in the news is spyware. It was not long ago that many people thought that "www" stood not for "World Wide Web," but for "Wild, Wild, Web." In this "Wild West," there appeared to be a modern gold rush fueled by advertising dollars, particularly the revenue from billions of pop-up ads. In the rush to get their ads in front of consumers, many advertisers ignored how their ads got there. Moreover, in the scramble to get ad-serving software onto millions of consumers' computers, some "spyware" and "adware" distributors failed to control or monitor the legions of affiliates they employed to distribute their software.

Let's say your client acquires a company that uses adware programs to advertise online. Should you be concerned? What should you look at? I would start with the FTC's two recent

settlements with major adware distributors Zango[13] and Direct Revenue.[14] In these settlements, the two companies agreed to disgorge a total of $4 million to settle FTC allegations that they installed their adware on consumers' computers without adequate notice or consent and deliberately made the programs difficult for consumers to remove. The consent orders establish basic ground rules regarding software downloads. First, a consumer's computer belongs to him or her, not to the software distributor. Second, buried disclosures of material information necessary to correct an otherwise misleading impression do not work, just as they have never worked in more traditional areas of commerce. Third, if a distributor puts a program on a consumer's computer that the consumer does not want, the consumer must be able to uninstall or disable it.

The broader underlying lessons here are that advertisers must be vigilant that their advertising dollars do not fund – either deliberately or inadvertently – illegal activity. And software distributors must be responsible for and need to closely monitor and carefully control their distribution systems.

Data security and spyware featured prominently in our Tech-Ade hearings, which many of you attended or watched online last November.[15] During four days of hearings, the Commission heard from 100 tech experts about the prospects for technological innovation, its

---

[13] *See* FTC Press Release, *Zango, Inc. Settles FTC Charges;* Will Give Up $3 Million in Ill-Gotten Gains for Unfair and Deceptive Adware Downloads (November 3, 2006), *available at* http://www.ftc.gov/opa/2006/11/zango.htm.

[14] *See* FTC Press Release, *DirectRevenue LLC Settles FTC Charges; Will Give Up $1.5 Million in Ill-Gotten Gains for Unfair and Deceptive Adware Downloads* (February 16, 2007), *available at* http://www.ftc.gov/opa/2007/02/directrevenue.shtm.

[15] *See* FTC Press Release, *Media Advisory; Protecting Consumers in the Next Tech-ade* (November 3, 2006), *available at* http://www.ftc.gov/opa/2006/11/techadema.shtm.

impact on consumers, and how the FTC could tailor its consumer protection policies in response over the next decade. The hearings covered topics from convergence to contactless payment; from demographic shifts to digital rights management; and from user generated content to ubiquitous computing. We intend to issue an FTC staff report this spring describing what we heard at the hearings. Then in the fall, we hope to host a series of Town Hall meetings around the country to supplement and expand on some of the key topics discussed at the hearings. We plan to consider what we hear at these meetings as part of the FTC staff's own internal strategic planning process, after which we will announce a Technology Research and Policy Development Plan for 2008.

IV. Health Advertising

Of course, not all recent consumer protection news has been focused on technology issues. Another headline-grabbing topic is America's obsession with health, fitness and psychological well-being. As consumers, these issues are important for you in your personal lives. As lawyers, you should be aware of legal standards that govern your clients' advertising of products touting health benefits for consumers. Whether your clients are entrepreneurs using infomercials, niche marketers advertising in specialized magazines, or large corporations airing ads during the Superbowl, the requirement is the same: Health claims must be backed up by sound science. Nobody gets a free pass on that requirement.

This past January, we announced settlements in four weight-loss cases, Xenadrine EFX, CortiSlim, TrimSpa, and Bayer One-A-Day WeightSmart.[16] In each of these cases, we alleged

---

[16] *See* FTC Press Release, *Federal Trade Commission Reaches "New Year's" Resolutions with Four Major Weight-Control Pill Marketers* (January 4, 2007), *available at* http://www.ftc.gov/opa/2007/01/weightloss.shtm.

that weight-loss or weight-control claims were not supported by competent and reliable scientific evidence. The four advertisers surrendered cash and other assets worth at least $25 million, and agreed not to make unsupported claims about their products.

In the Bayer case, we obtained a $3.2 million civil penalty payment, which is the largest ever obtained by the Commission in a health claims case. The product at issue, One-A-Day WeightSmart, was a multivitamin, not merely a weight-control product. It contained a sprinkling of green tea extract, the purported weight control ingredient.

The settlement stands for several propositions. First, any health claim, regardless of other uses or benefits of a product, requires competent and reliable scientific evidence for the claimed benefit. Second, the dosage and combination of a product's active ingredients that have been tested must be similar to the those found in the actual product. Third, companies that are already under order, like Bayer was, have a particular obligation to make sure that the science matches the claims. And finally, advertising law principles apply equally to large national advertisers as they do to smaller marketers.

I can't leave the health advertising topic without mentioning our case involving the Q-Ray pain relief bracelet.[17] In that case, the defendants used a massive infomercial campaign to sell bracelets that purportedly provided immediate, significant or complete pain relief. After a seven-day trial, the court found these claims were not backed up with sound science. The court further explained that competent and reliable scientific evidence for such pain relief claims needed to consist of at least one well-conducted, placebo-controlled, randomized, double-blind

---

[17] *See* FTC Press Release, *Court Rules in FTC's Favor in Q-Ray Bracelet Case; Orders Defendants to Pay Up To $87 Million* (September 20, 2006), *available at* http://www.ftc.gov/opa/2006/09/qray.shtm.

clinical study.

Defendants claimed that consumers got their money's worth from the product because they benefitted from its placebo effect. The court debunked that defense, noting that for a placebo to work, "the consumer must be duped." The court ordered the defendants' to pay up to $87 million in refunds to consumers. The lesson from this case is clear: For those of you ever thinking of employing the "placebo effect" defense: forget it.

IV. Conduct of Affiliates

Let me mention another important lesson that comes up repeatedly in our consumer protection cases: Monitor the conduct of your affiliates. Let's say a client comes to your office and says, "I hire affiliates to do my advertising and marketing campaigns. I use offshore call centers to telemarket to consumers and process customer data. Am I off the hook?" Of course, the answer is no.

Many of our cases involve companies who turn a blind eye to their affiliates' activities. I've already talked about Direct Revenue and Zango. Last year, we announced a $5.3 million civil penalty against DirecTV, charging that it and the companies it hired violated the Do Not Call provisions of the Commission's Telemarketing Sales Rule.[18] Similarly, a majority of our CAN SPAM Act cases did not target those who actually pushed the button to send the spam, but those who hired spammers to conduct their marketing campaigns.[19]

Any company subject to the FTC's jurisdiction is responsible for complying with the laws

---

[18] *See* FTC Press Release, *DirecTV to Pay$5.3 Million Penalty for Do Not Call Violations* (December 13, 2005), available at http://www.ftc.gov/opa/2005/12/directv.shtm.

[19] *See* e.g., FTC Press Release, *FTC Slams Spammer in Pocketbook; "FreeFlixTix" Scheme Threatened Reliability of E-mail* (March 23, 2006), *available at* http://www.ftc.gov/opa/2006/03/freeflixtix.shtm.

we enforce. Simply because a company chooses to outsource some of its functions does not allow it to escape liability. This is true regardless of whether the affiliate is foreign or domestic. If you outsource functions to a foreign service provider, and the provider loses American consumers' data or calls Americans on the Do Not Call registry, you can be sure that we will come knocking on your door.

V. Conclusion

I have provided you with a snapshot of how we have been addressing the major consumer protection issues of our day. Of course, there are many more important consumer protection issues in the headlines, ranging from subprime lending to social networking, which I have not covered today. You can read about our activities in these and other areas in the FTC's Annual Report, as well as in your daily newspapers. Thank you for your attention, and I would be happy to answer any questions.